DII.COE.Final.HP1020.SAM

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

System Administrator’s Manual (SAM) for SPI, version 1.0.0.2

Document Version 1.0.0.2

27 August 1997

Prepared for:

Defense Information Systems Agency

Prepared by:

NRaD
San Diego, CA

Table of Contents

This page intentionally left blank.

1. Scope

1.1 Identification

This System Administrator's Manual (SAM) document is for SPI (segprefix SPI322) Version 1.0.0.2 for the HP10.20 Platform. It provides system administrators specific guidance to support COE system and software installation and maintenance.

1.2 System Overview

This version of SPI (The Distributed Security Profile Inspection System) provides the capability to conduct simultaneous inspections of the UNIX hosts of a security domain from a central control point called the Command Center. Inspections may be performed on demand, and may also be scheduled to run automatically on a regular basis.

2. Referenced Documents

Installation Procedures (IP) for SPI version 1.0.0.2, 27 August 1997.

3. Operating Guidelines

The default behavior of this software is to run from a UNIX prompt..

Various capabilities of SPI-NET can be found in Appendix A.

4. Installation Overview

This version of SPI can be installed in accordance with the Installation Procedures document for SPI version 1.0.0.2.

5. System Administration Utilities

None.

6. Operation/Maintenance Procedures

None.

7. Error Recovery Guidelines

To shutdown the SPI processes, type ps -ef at the root prompt to list all of the current processes. Locate the SPI processes and its process number. Once you have located that number, execute the following:

```
# kill -9 <process number>
```

This will immediately kill the SPI process. To restart SPI, execute the following at the root prompt:

```
# /h/COE/Comp/SPI/bin/spin-97.06A/binr/StartRCS
# /h/COE/Comp/SPI/bin/SPI_spinet
```

8. Notes

None.

A. Appendices

```
============================================================
PLEASE READ THE FILE "ACCESS POLICY" FOR INFORMATION DETAILING
YOUR RESPONSIBILITIES WITH REGARD TO SPI-NET REDISTRIBUTION.
============================================================

Welcome to SPI-NET Installation
-------------------------------

This README file contains instructions for installing both the SPI-NET
source packages as well as the SPI-NET binary (pre-compiled) packages.
Please refer to the appropriate section below for details.

------------------------------------
UNPACKING THE ORIGINAL DISTRIBUTION:
------------------------------------

You will need to use des, uncompress and tar to unpack your distribution.
You will need a des keyvalue to decrypt the package.

Example:
   des -d -k keyvalue < spin(version).tar.Z.des > spin(version).tar.Z
   uncompress spin(version).tar.Z
   tar -xvf spin(version).tar
```

If you are installing a source-code version, you will find there is now an "Install" script and another large tar file. Do not un-tar the inner tar file. The Install script expects it to be there.

If you are installing a binary (pre-compiled) version, you will now have a directory called "spin(version)". cd into this directory and run the script called "Setup" to complete the installation.

INSTRUCTIONS FOR SOURCE INSTALLATION:

The supplied "Install" script is responsible for determining your system configuration and properly installing the SPI-NET components.

"Install" will expect to find at least one SPI-NET (source) distribution tar file in the same directory where the Install script resides. If more than one such tar file exists, it will prompt you to select the desired package. See "About The New SPI-NET Distributions" below for details.

** Please do not un-tar and remove the file manually prior to
** running the Install script. The Install script will take care
** of un-tarring the selected file and processing the components.

Simply type "Install" (or ./Install) to start the installation.

Toward the end of the configuration phase, you will be asked to indicate which host is to be your Command Host. If you are installing the Master Source code (spinS-version), indicate the name of the host where you are now doing the installation. If you are installing a Remote Source code (spinRS-version), indicate the name of the host that will be the Command Host for your SPI-NET security domain. In this case, you will also be asked to supply a (up to) six-digit number, uniquely identifying this host to your Command Host.

Note: For SPI-NET Remote (non-Command-Host) installations, you will need to obtain DSS key certificates from your Command Host. See your Command Host operator for details.

After installation is complete, see the section "STARTING SPI-NET".

INSTRUCTIONS FOR BINARY INSTALLATION:

There is a "SetUp" script in the binary distribution package. It is responsible for determining your client/server environment configuration, and properly set up the communication host table value.

Simply type "SetUp" (or ./SetUp) to complete the installation.

Setup will ask you which host is to be your Command Host. If it is the host you are currently installing SPI-NET, you will be assigned SPI-NET HostID HID_000001. Otherwise, it will prompt you to enter a unique (up to) six-digit number from which it will form a SPI-NET HostID.

(SetUp configures your binm and/or binr D/HOSTINFO/Host_Table.)

Note: For SPI-NET Remote (non Command Host) installations, you will need to obtain DSS key certificates from your Command Host. See your Command Host operator for details.

After installation is complete, see the section "STARTING SPI-NET".

STARTING SPI-NET

Once installation is completed, perform the following operation(s):

> NOTE: If you are already running SPI_NET JCS, MCS, or RCS from a previous install, you will need to kill them prior to starting up new ones, to avoid a port-assignment conflict. You may use "ps | grep csx" to see if any of jcsx, mcsx, or rcsx are active.

a) For the Command Host Package ...

> cd to (spin-version)/binr, and type ./StartRCS
>
> cd to ../binm and type ./spinet

When the SPI-NET UI appears, you will be prompted to enter an initial password. After this, two dialogs will appear, explaining that the

Master Communication Server (MCS) and Job Control System (JCS) are down. Select "Restart" in each case.

When you install SPI-NET Remote Packages on other hosts, you will need to add them to the Command Host Security Domain. To do so, select "Domain: Assign HostIDs" to add these hosts to the Host_Table. Then select "Domain: DSS Certificates", select the newly added hosts, and use the "Generate/Assign Certificates" button to generate keys. These key files will reside in binm/D/CERTINFO/ISSUED. You will need to ftp the crt_000001.pub certificate and the appropriate private (crt_??????.prv) certificate to the binr/D/CERTINFO directory on each SPI-NET Remote Host. (On the Command Host, this operation will occur automatically.)

Use the provided Help system documentation to proceed thereafter.

b) For each Remote Host Package ...

cd to (spin_rb-version)/binr and type ./StartRCS

===================================

About The New SPI-NET Distributions

===================================

The new SPI-NET distributions come in 4 "Top-Level" packages:

spinS-(version).tar.Z.des - - - - - Full Source Package

spinRS-(version).tar.Z.des - - - - - Remote Source Package

spin.b-(version).(OS_Type).tar.Z.des - - Full Binary Package

spin.rb-(version).(OS_Type).tar.Z.des - - Remote Binary Package

The Similarities:

The two source packages, when un-tarred, will contain an "Install" script as well as another large tar file. The Install script will take care of un-tarring the "inner" tar file and provide the user with certain options regarding installation appropriate to the packages contained within.

The two types of binary packages, when untarred, will create a directory of the form "spin(version)/". In this directory you will find a script called "SetUp" which will configure the SPI-NET environment.

The Differences:

The Full Source Package (spinS) has the capability of reproducing itself, (spinS) and any of the other packages. Simply answer "yes" when asked if you wish to create a "Production" environment. Of course, it can only make Binary packages (spinB or spin.rb) for systems upon which it is installed.

Only the Full Source (spinS) or Full Binary (spin.b) packages contain the Command Host utilities, user interface, etc, needed for SPI-NET operation.

The Remote Packages (spinRS and spin.rb) have no Command Host capability, and their operation must be directed from a designated Command Host system.

Either the Full Source (spinS) or Remote Source (spinRS) may be used to create a multiply-installable Remote Binary package (spin.rb).

NOTES:

For any SPI-NET security domain, there must be exactly one Command Host. It will be given the SPI-NET HostID "HID_000001". All the remote hosts must be assigned unique HostIDs "HID_nnnnnn" where nnnnnn is not 000001.

On a Command Host, Install will automatically build the Command Host utilities and the Remote utilities, enabling self-inspection. There is no need to separately install the Remote Package (spinRS or spin.rb) on a Command Host.

Remote Hosts intended as inspection targets for a given Command Host must must have a Remote Package (spinRS or spin.rb) installed. At installation time, you will be prompted to assign a unique "nnnnnn" for a HostID, and you will be asked to give the ordinary hostname of the machine that will be acting as Command Host for that remote system.

Use the Command Host utility to generate DSS public keys for any Remote (non-Command-Host) SPI-NET systems, and distribute the public and private key members to Remote systems according to the online documentation.

All SPI-NET DSS key certificates (crt_nnnnnn.prv and crt_nnnnnn.pub) must have the 6-digit "nnnnnn" correspond to the appropriate SPI-NET HostID. The Command Host should have its own crt_000001.prv, and the crt_nnnnnn.pub for each remote SPI-NET HostID HID_nnnnnn. Each remote host must have its own crt_nnnnnn.prv, and the crt_000001.pub of the CommandHost.

=====================================
DESCRIPTION OF THE SOURCE DIRECTORIES

=====================================

For those who are installing the SPI-NET from source, here is a brief description if the source directories:

"srcm"

Contains source code for the SPI-NET Master Utilities such as the user interface, job control system (JCS), report manager (RPM), and the secure communication agents (MCC and MCS). In addition, there is source for DES and DSS certificate generation.

"srcr"

Contains source code for the SPI-NET Remote Inspection tools (act, bat, cdt, cql, psi, qsp,) the remote job monitor (RJM), and the remote (client/server) secure communication agents (RCC and RCS).

"srcl" and "include"

Contains source code libraries for functions common to the Master utilities (srcm) and the Remote tools (srcr.)

"tcltk"

This directory contains the tcl-tk source code needed for the SPI-NET user interface, automatically installed.

When you build a complete SPI-NET (via the Install script,) ALL of the above codes are compiled and installed on the local system (generally referred to as the Command Host). This includes the remote inspector tools and com-agents. This way, self-inspection of the local system occurs just as if it were another remote inspection target.

This page intentionally left blank.